# EU-Datenschutz-Grundverordnung
## Leitfaden

Die Datenschutz-Grundverordnung regelt den Umgang mit personenbezogenen Daten. Die Neuerungen betreffen nicht nur Ihr Unternehmen, sondern auch Sie persönlich. Dieser Leitfaden informiert Sie über die wesentlichen Aspekte und die wichtigsten Handlungserfordernisse des Datenschutzes in Ihrem Unternehmen.

# EU-Datenschutz-Grundverordnung

Die neue Datenschutz-Grundverordnung (DSGVO) führt mit ihren 99 Artikeln und 173 Erwägungsgründen erstmals unmittelbar geltendes, europaweit einheitliches Datenschutzrecht für Unternehmen, Privatpersonen und die öffentliche Verwaltung ein.

Die Auswirkungen sind keinesfalls zu unterschätzen. Die Anforderungen zwingen zu einem grundlegenden rechtlichen Umdenken und zu einer weitgehenden Neuausrichtung der bisherigen Datenschutzkonzepte.

Das Thema Datenschutz betrifft von jeher jeden. Wir alle haben sowohl Rechte bezüglich unserer eigenen Daten als auch Pflichten, z. B. bei der Verarbeitung der Daten unserer Kunden.

Mit der Digitalisierung gewinnt der Datenschutz jedoch an Bedeutung: Datenverarbeitung, Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse werden immer einfacher und damit auch immer machbarer. Datenverarbeitung greift in fast alle Bereiche unseres Lebens ein und gibt bereits heute in vielen Dingen die Richtung vor. In unser aller Interesse darf dies nicht unkontrolliert geschehen. Die DSGVO ist ein Ausdruck dieser Entwicklung.

**173 Erwägungsgründe**
Die der DSGVO vorangestellten Erwägungsgründe spiegeln die Vorüberlegungen zur DSGVO: Sie demonstrieren eindrucksvoll die Komplexität und auch die deutlich gestiegene Bedeutung des Datenschutzes in der Informationsgesellschaft.
[https://dsgvo-gesetz.de/erwaegungsgruende/]

**Schutzziel**
„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten."
(Art. 1 Abs. 2 DSGVO)

Mit dem Schutzbedarf steigt der Regelungsbedarf. Insbesondere gilt es, das informationelle Selbstbestimmungsrecht des Einzelnen zu schützen. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich nur auf der Basis gesetzlicher Vorschriften oder der Einwilligung der betroffenen Person zulässig. Ein verantwortungsvolles Handeln im Umgang mit personenbezogenen Daten ist jedermanns Aufgabe, über alle Hierarchieebenen und Funktionen hinweg.

Der vorliegende Leitfaden wurde mit größtmöglicher Sorgfalt erstellt, erhebt jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit und ersetzt inbesondere keine fundierte, rechtliche Beratung zu den einzelnen Themenfeldern. Er will insoweit für den Datenschutz sensibilisieren, Rechte und Pflichten im Arbeitsumfeld veranschaulichen und einen ersten Eindruck über die neue DSGVO verschaffen.

# Datenschutzrelevante Gesetze

### Europäische Gesetzgebung

Die **EU-Datenschutz-Grundverordnung** (DSGVO) enthält die neuen, europaweit gültigen Vorschriften zum Datenschutz. Nationale Regelungen dürfen nichts Gegenteiliges regeln. Aber an einigen Stellen müssen bzw. dürfen die nationalen Gesetzgeber ergänzende und detailliertere Vorschriften erlassen („Öffnungsklauseln"), z. B. zum Datenschutz der Beschäftigten, des öffentlichen Sektors und der Kirchen.

Die daneben stehende **EU-Datenschutzrichtlinie 2016/680** enthält spezielle Regelungen für Justiz und Polizei. Als europäische Richtlinie muss sie in nationales Recht umgesetzt werden.

### Nationale Gesetzgebung

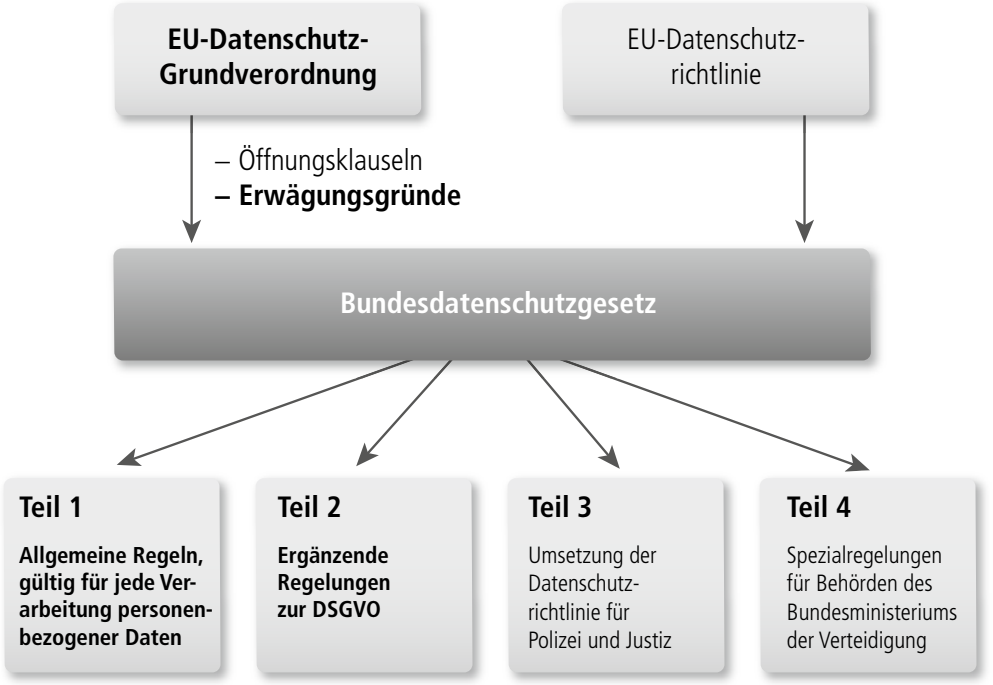
Das neue Bundesdatenschutzgesetz (BDSG-neu) enthält

- ergänzende, konkretisierte und modifizierte Regeln zur DSGVO,
- die nationale Umsetzung der EU-Datenschutzrichtlinie (BDSG-neu Teil 3) sowie
- weitere Ergänzungen.

Für Unternehmen und damit auch für Sie als Mitarbeiter sind insbesondere Teil 1 und Teil 2 BDSG-neu (siehe Abbildung) von Bedeutung.

Daneben gibt es noch eine Reihe weiterer Gesetze auf Bundes- und Landesebene, die Bezug zum Datenschutz haben und ebenfalls beachtet werden müssen, z. B.

- das Telekommunikationsgesetz,
- die Sozialgesetze,
- das Kunsturhebergesetz,
- das Gesetz gegen den unlauteren Wettbewerb oder auch
- einzelne Paragrafen aus dem BGB sowie
- dem StGB (z. B. § 203 StGB, Verletzung von Privatgeheimnissen).



# Datenverarbeitung

Die DSGVO verlangt die Rechtmäßigkeit der Datenverarbeitung und macht gezielte Vorgaben, wann die Verarbeitung personenbezogener Daten rechtmäßig ist (Art. 5 DSGVO).

Die Verarbeitung von personenbezogenen Daten meint nach Art. 4 Nr. 2 DSGVO:
„… *das Erheben*, *das Erfassen*, *die Organisation*, *das Ordnen*, *die Speicherung*, *die Anpassung oder Veränderung*, *das Auslesen*, *das Abfragen*, *die Verwendung*, *die Offenlegung durch Übermittlung*, *Verbreitung oder eine andere Form der Bereitstellung*, *den Abgleich oder die Verknüpfung*, *die Einschränkung*, *das Löschen oder die Vernichtung*."

**Praxistipp**
Die DSGVO gilt für Papierunterlagen ebenso wie für elektronisch vorgehaltene Daten. Wichtig an dieser Stelle ist, dass sie eine gewisse Systematik aufweisen müssen, die ein schnelles „Überblicken" der vorhandenen Daten ermöglicht. Ein unsortierter Schreibtisch würde also nicht unter die DSGVO fallen.

Entscheidend ist, dass eine Ordnung nach bestimmten Kriterien erfolgt. Wenn dies der Fall ist, fallen auch Akten oder Aktensammlungen in den Anwendungsbereich der DSGVO (Erwägungsgrund 15: Technikneutralität).

Datenverarbeitung hat auf „rechtmäßige" Weise, nach „Treu und Glauben" und in einer für die betroffene Person „nachvollziehbaren Weise" (Transparenz) zu geschehen.
Eine Datenverarbeitung muss immer zweckgebunden und angemessen, auf das notwendige Maß beschränkt, sachlich begründet, richtig und aktuell erfolgen. Es dürfen immer nur so viele Daten wie unbedingt erforderlich verarbeitet werden.

Die Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für den jeweiligen Zweck erforderlich ist. Schlussendlich muss der Datenverarbeiter eine angemessene Sicherheit der personenbezogenen Daten gewährleisten können.

**Voraussetzung**
Eine Verarbeitung personenbezogener Daten ist weiter nur dann rechtmäßig, wenn zusätzlich mindestens eine der nachstehenden Bedingungen erfüllt ist:

**a. Einwilligung**
Die Verarbeitung personenbezogener Daten ist zulässig, wenn die betroffene Person ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gibt (Art. 6 Abs. 1 lit. a DSGVO). Dabei muss der Datenverantwortliche seiner Nachweispflicht entsprechen. Darüber hinaus hat er darauf zu achten, dass die Einwilligung jederzeit und auf einfache Weise widerrufen werden kann.

**Aus der Praxis**
Die Einwilligungserklärung ist der „schwächste" Erlaubnistatbestand, weil er jederzeit widerrufen werden kann. Praktische Anwendung findet er beispielsweise bei der Veröffentlichung von Mitarbeiterfotos im Internet. Eine gute Orientierung, wie so eine Einverständniserklärung aussehen kann, finden Sie im Internet, z. B. auf den Internetseiten der Landesbeauftragten für den Datenschutz.

**b. Erfüllung eines Vertrages**
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn
- ▷ sie für die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei die betroffene Person ist, oder
- ▷ sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 lit. b DSGVO).

In der Praxis spielt diese Regelung beispielsweise beim Vertragsabschluss eine Rolle. Ein anderes Beispiel ist, wenn die betroffene Person (z. B. ein Kunde) einen entsprechenden Antrag gegenüber dem Datenverantwortlichen (z. B. einer Bank) stellt, um einen Vertrag (z. B. einen Kreditvertrag) vorzubereiten bzw. zu verhandeln.

**c. Erfüllung einer rechtlichen Verpflichtung**
Hierunter fallen unter anderem Sozialversicherungsrecht, Abgabenordnung oder Telekommunikationsrecht.

**d. Schutz lebenswichtiger Interessen**

**e. Öffentliches Interesse**
Die Verarbeitung personenbezogener Daten kann auch dann zulässig sein, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 lit. e DSGVO und Erwägungsgrund 45). Dazu bedarf es jedoch einer rechtlichen Grundlage.

**f. Legitime Interessen/Interessenabwägung**
Eine Verarbeitung personenbezogener Daten kann auch dann zulässig sein, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Voraussetzung ist allerdings, dass diese schwerer wiegen als die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person.

**Aus der Praxis**
Eine Auftragsverarbeitung liegt beispielsweise vor, wenn Sie in einer Druckerei ein Mailing erstellen lassen. Bei der Erstellung und Durchführung des Mailings greift die Druckerei auf personenbezogene Daten Ihrer Kunden (z. B. Name, Adresse) zurück. Damit auch hier der Datenschutz gewährleistet ist, trifft Ihr Unternehmen mit der Druckerei eine Vereinbarung (Vertrag zur Auftragsverarbeitung).

### Auftragsverarbeitung

Der Begriff der Auftragsverarbeitung löst den bisher verwandten Begriff der „Auftragsdatenverarbeitung“ ab. Eine Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (Auftragnehmer)

- nach Weisung und
- im Auftrag des Verantwortlichen (Auftraggeber).

Wenn Verarbeitungen ausgelagert werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung hilft dem Unternehmen dabei, Haftungsrisiken vorzubeugen.

# Zusammenspiel

**Pflichten von Unternehmen als Verantwortliche**
(s. a. Seite 7)

- Rechtmäßigkeit der Datenverarbeitung
- Transparenz
- Richtigkeit der Daten
- Schadensersatz
- Sicherstellung des Datenschutzes durch angemessene Technik

**Rechte von natürlichen Personen als Betroffene**
(s. a. Seite 10)

- Auskunft über gespeicherte Daten
- Berichtigung der Daten
- Löschen und Sperren der Daten
- Datenportierung

**Aufgaben des Staates/der Aufsichtsbehörden**
(s. a. Seite 12)

- Kontrolle der Unternehmen
- Verhängen von Bußgeldern
- Ansprechpartner für betroffene Personen und Unternehmen

**Bei Verstößen drohen sowohl Unternehmen als auch ihren Mitarbeitern empfindliche Konsequenzen** (Seite 13).

**Der Datenschutzbeauftragte nach DSGVO und BDSG-neu**
Der Datenschutzbeauftragte hat folgende Aufgaben:

- Analyse und Bewertung der Risikosituation des Unternehmens mit Blick auf den Datenschutz
- Unterrichtung und Beratung des Verantwortlichen und seiner Mitarbeiter
- Mitwirkung an der Datenschutz-Folgenabschätzung
- Überwachung der Einhaltung der rechtlichen Vorgaben
- Zusammenarbeit mit Behörden
- Ansprechpartner für alle Mitarbeiter eines Unternehmens in Sachen Datenschutz

# Pflichten von Unternehmen

Unternehmen haben nach der DSGVO zahlreiche Pflichten. Zu den wichtigsten zählen:

**I. Grundsätze der Verarbeitung personenbezogener Daten**
**II. Transparenzpflichten**
**III. Rechenschaftspflicht**
**IV. Meldepflicht bei Datenpannen**
**V. Schadensersatz**

## I. Verarbeitungsgrundsätze

1. **Verarbeitung nach Treu und Glauben** (Art. 5 Abs.1 lit. a, Erwägungsgrund 39)
   Die personenbezogenen Daten dürfen nur so verarbeitet werden, wie es bei der Erhebung angegeben wurde. Es geht allgemein um den redlichen und ehrlichen Umgang mit den Daten.
2. **Zweckbindung**
   Der Zweck muss vor der Verarbeitung festgelegt werden. Er muss eindeutig und rechtmäßig sein. Sollen die Daten zu einem anderen Zweck weiterverwendet werden, muss es einen Rechtfertigungsgrund geben.
3. **Datenminimierung**
   Die Daten müssen für den Zweck angemessen und relevant sein. Sie müssen sich auf die notwendigen Informationen beschränken.
4. **Richtigkeit**
   Es muss gewährleistet sein, dass die Daten richtig und auf dem neuesten Stand sind. Unrichtige Daten müssen umgehend korrigiert oder gelöscht werden.
5. **Speicherbegrenzung**
   Daten dürfen nicht länger verarbeitet werden, als es für den Zweck, für den sie erhoben wurden, notwendig ist. Danach sind sie zu löschen.
6. **Integrität und Vertraulichkeit**
   Daten sind vor unrechtmäßiger Verarbeitung durch Unbefugte und vor unbeabsichtigter Beschädigung und Verlust zu schützen.

## II. Transparenzpflichten

### 1. Informationspflichten

- Unternehmen haben umfangreiche Informationspflichten gegenüber betroffenen Personen, wenn sie deren Daten verarbeiten. Die DSGVO unterscheidet dabei zwischen
  - direkter (Art. 13 DSGVO) und
  - indirekter Erhebung (Art. 14 DSGVO) sowie
  - der Informationspflicht bei Berichtigung oder Löschung (Art. 19 Abs. 2 DSGVO).

  Wenn Daten indirekt, also bei Dritten, erhoben werden, müssen die betroffenen Personen auf den gleichen Informationsstand gebracht werden, wie wenn die Daten direkt erhoben worden wären. Hinzu kommt die Quellenangabe.

**Aus der Praxis**

Die **Aufbewahrungsfristen** und damit auch die **Löschfristen** werden durch die jeweiligen Gesetze, z. B. das Handelsgesetzbuch (HGB), oder etwa durch steuerrechtliche Vorgaben geregelt.

Wenn beispielsweise das HGB eine Aufbewahrung über sechs Jahre hinweg vorsieht, müssen nach Ablauf der sechs Jahre alle zu diesem Zweck erhobenen Daten gelöscht werden.

Genauso verhält es sich mit der **Datenerhebung.** Auch hier sind die gesetzlichen Bestimmungen maßgeblich. Es dürfen nur Daten erhoben und gespeichert werden, die zwingend erforderlich sind.

Beispielsweise mag für eine Kreditvergabe entscheidend sein, ob jemand – umgangssprachlich ausgedrückt – „auf großem Fuß" lebt. Dennoch ist es nicht legal, Daten zur Schuhgröße zu erfassen. Diese Daten sind im Sinne des Gesetzes unerheblich für den Geschäftsvorgang – und dürfen deshalb auch nicht erhoben bzw. verarbeitet werden.

- Weitere wichtige Informationspflichten haben Unternehmen bezüglich des Hinweises auf das Widerspruchsrecht (Art. 21 Abs. 4 DSGVO) und der Benachrichtigung von Personen, die von einer Datenpanne betroffen sind (Art. 34 DSGVO).

**2. Auskunftspflicht**

Auf Verlangen muss ein Unternehmen den betroffenen Personen kostenlos Auskunft erteilen über

- die gespeicherten Daten,
- die Herkunft und die Empfänger der Daten,
- den Zweck der Speicherung sowie
- die Rechte der betroffenen Personen.

## III. Rechenschaftspflicht

Entsprechend der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO muss der Verantwortliche jederzeit nachweisen können, dass die Datenverarbeitung rechtskonform erfolgt.

Dazu muss dokumentiert werden, wie das Unternehmen die Einhaltung des Datenschutzes gewährleistet.

Besondere Bedeutung haben in diesem Zusammenhang das Verzeichnis von Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung.

**Dokumentation**
Mit der DSGVO ändert sich der Stellenwert der Dokumentation. Sie dient dem Nachweis, dass die gesetzlichen Vorschriften eingehalten werden.

**Verzeichnis von Verarbeitungstätigkeiten**

Die Übersicht dient dazu, alle in einem Unternehmen eingesetzten Verfahren zur Verarbeitung personenbezogener Daten aufzulisten und deren Zweck zu dokumentieren.
In dem Verzeichnis müssen für jedes Verfahren folgende Punkte beschrieben werden:

- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die die personenbezogenen Daten übermittelt werden
- Übermittlungen von Daten an ein Drittland außerhalb der EU
- Fristen für die Löschung der Daten
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
- Bewertung der Risiken der Datenverarbeitung für die betroffenen Personen

**Datenschutz-Folgenabschätzung (DSFA)**

Datenverarbeitungen, die mit einem besonders hohen Risiko für die betroffenen Personen verbunden sind, müssen genauer betrachtet werden.

Dies muss vor dem ersten Einsatz geschehen und danach regelmäßig bei Änderungen am Verfahren. In der Praxis ist die Beurteilung schwierig, ob ein Verfahren mit besonders hohen Risiken verbunden ist.

Art. 35 Abs. 3 DSGVO nennt hierzu einige Faktoren, die wahrscheinlich zu einem hohen Risiko (Art. 35 Abs. 1 DSGVO) führen. Die Datenschutz-Aufsichtsbehörden wollen hierzu noch nähere Angaben machen (Black- und White-Listen).
Auf alle Fälle gehören aber folgende Verfahren dazu:

- Automatisierte Bewertung persönlicher Aspekte: Beispiele sind das Scoring für eine Kreditentscheidung oder auch Persönlichkeitstests bei Bewerbern.
- Verarbeitung besonders sensibler Daten (Art. 9 Abs. 1 DSGVO): Biometrische Daten zur Personenerkennung (Fingerabdruck, Gesichtserkennung) würden beispielsweise darunterfallen.
- Videoüberwachung in öffentlich zugänglichen Bereichen: Hierzu zählen Einkaufszentren, Bahnhöfe, Flughäfen und auch der SB-Bereich von Banken.

## IV. Meldepflicht bei Datenpannen

Kommt es zu einem Verstoß gegen den Datenschutz, hat das Unternehmen insbesondere zwei Meldepflichten:

**1. Gegenüber der Aufsichtsbehörde**
(Art. 33 DSGVO)
Die Meldung hat innerhalb von 72 Stunden zu erfolgen, wenn ein Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen besteht.

**2. Gegenüber der betroffenen Person**
(Art. 34 DSGVO)
Die Meldung ist dann erforderlich, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen besteht

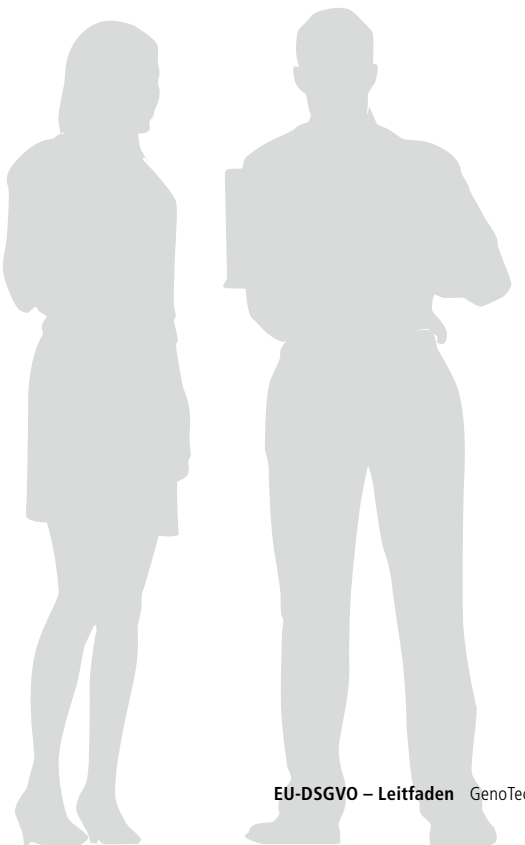
Beispiele für Datenpannen, die ggf. gemeldet werden müssen:

- Verlust/Diebstahl eines USB-Sticks mit unverschlüsselten Kundendaten
- Versehentlicher elektronischer Versand einer unverschlüsselten Liste mit Kundendaten an einen unrechtmäßigen Empfänger
- Hackerangriff mit Abzug von Daten

## V. Schadensersatz

Schließlich ist das Unternehmen als Verantwortlicher zum Ausgleich des durch einen Verstoß gegen diese Verordnung entstandenen materiellen wie immateriellen Schadens beim Betroffenen verpflichtet.

**Achtung! Der Datenschutzbeauftragte sollte immer eingeschaltet werden.**
Die Beurteilung, ob es sich bei einem Vorfall um eine Datenschutzpanne handelt oder nicht, ist nicht immer einfach. Deshalb wird empfohlen, die Bewertung durch den Datenschutzbeauftragten vornehmen zu lassen. Dieser kann dann auch gleich Maßnahmen zur Einschränkung des Risikos vornehmen.



# Rechte betroffener Personen

Die DSGVO räumt den betroffenen Personen (Kunden, Mitarbeitern etc.) zahlreiche Rechte ein, die sich wie folgt aufschlüsseln lassen:

- **Permissionsrechte**
  Sie gestatten Datenverarbeitungen, die an sich unzulässig wären (z. B. durch Einwilligung).
- **Interventionsrechte**
  Sie verhindern bestimmte Datenverarbeitungen
- **Informationsrechte**
  Sie informieren darüber, was mit den Daten passiert.
- **Kompensationsrechte**
  Sie gleichen entstandenen Schaden durch Entschädigung aus.
- **Petitionsrechte**
  Sie stellen sicher, dass und an wen sich die betroffene Person bei Fragen zum Datenschutz wenden kann.

Im Detail hat die betroffene Person folgende, nicht abschließend aufgeführte Rechte:

### Interventionsrechte

**Recht auf Widerspruch** (Art. 21 DSGVO)
Die betroffene Person kann der weiteren Verarbeitung ihrer personenbezogenen Daten widersprechen. Der Verantwortliche und mögliche weitere Datenempfänger müssen dann die Verarbeitung einstellen. Das Widerspruchsrecht gilt insbesondere bei Direktwerbung (Art. 21 Abs. 2 DSGVO).

**Recht auf nicht ausschließlich automatisierte Entscheidungen** (Art. 22 DSGVO)
Entscheidungen, die gegenüber einer betroffenen Person rechtliche Wirkung entfalten oder sie in sonstiger Weise erheblich beeinträchtigen, dürfen grundsätzlich nicht ausschließlich automatisiert getroffen werden. Beispielsweise darf ein beantragter Kredit nicht allein aufgrund mathematischer Algorithmen gewährt oder abgelehnt werden. Es sei denn, der Betroffene hat hierin ausdrücklich eingewilligt oder andere Erlaubnistatbestände liegen vor.

**Information und Kommunikation**
Art. 12 und 13 der DSGVO besagen, dass die betroffenen Personen immer über die Verarbeitung transparent und verständlich zu informieren sind.

**Recht auf Berichtigung** (Art. 16 DSGVO)
Fehlerhafte Daten muss der Verantwortliche korrigieren, wenn die betroffene Person es verlangt. Wurden die Daten an Dritte weitergegeben, müssen auch diese informiert werden.

**Recht auf Löschung** (Art. 17 DSGVO)
Betroffene Personen können verlangen, dass der Verantwortliche und mögliche weitere Datenempfänger ihre personenbezogenen Daten löschen. Dies gilt allerdings nur, wenn die weitere Verarbeitung nicht mehr erforderlich oder gesetzlich vorgeschrieben ist. Sobald der Zweck oder die Rechtsgrundlage der Verarbeitung entfällt, ist jede weitere Verarbeitung unzulässig und die Daten müssen gelöscht werden.

**Recht auf Einschränkung** (Art. 18 DSGVO)
Können Daten nicht gelöscht werden, z. B. weil es gesetzliche Aufbewahrungsfristen gibt, kann die Verarbeitung eingeschränkt werden. Der Verantwortliche kann solche Daten mit einem Sperrvermerk versehen.

### Informationsrechte

**Recht auf transparente Information und Kommunikation** (Art. 12 DSGVO)
Die Kommunikation hat in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

**Recht auf Information** (Art. 13 und 14 DSGVO)
Jede betroffene Person erhält die ihr zustehende Information und zwar schon vor der Datenverarbeitung und ohne danach fragen zu müssen.
Die DSGVO unterscheidet zwischen

a. der Erhebung unmittelbar bei der betroffenen Person und
b. der Erhebung durch einen Dritten, z. B. Adresshändler, Verbundpartner.

Auf die Information bei direkter Erhebung oder Erhebung durch Dritte kann nur verzichtet werden, wenn die betroffene Person bereits alle Inhalte, die unter die Informationspflicht fallen, kennt.

**Recht auf Auskunft** (Art. 15 DSGVO)
Auf Anfrage muss das Unternehmen den betroffenen Personen mitteilen,

a. welche Daten zu der Person wo und wie verarbeitet werden,
b. woher sie stammen,
c. wohin sie übermittelt werden und
d. wie lange die Daten verarbeitet oder aufbewahrt werden.

**Recht auf Benachrichtigung bei Datenpannen** (Art. 34 DSGVO)
Kommt es bei der Verarbeitung zu Datenpannen (Rechtsverletzungen), so hat der Betroffene das Recht auf eine entsprechende Mitteilung. Zusätzliche Voraussetzung ist jedoch, dass hierdurch ein hohes Risiko für die Rechte und Freiheiten des Betroffenen besteht.

**Recht auf Datenübertragbarkeit** (Art. 20 DSGVO)
Betroffene Personen können verlangen, dass der Verantwortliche ihre personenbezogenen Daten in einem strukturierten und maschinenlesbaren Format zur Verfügung stellt. Übrigens: Wenn der Verantwortliche diese Daten um eigene Erkenntnisse und Erfahrungen ergänzt hat, so unterliegen diese Aufzeichnungen nicht diesem sogenannten „Portabilitätsanspruch".

### Kompensationsrechte

**Recht auf Schadensersatz** (Art. 82 DSGVO)
Schließlich kann die betroffene Person, der aufgrund eines Verstoßes gegen die Verordnung ein matiereller oder immaterieller Schaden entstanden ist, Schadensersatz geltend machen.

### Petitionsrechte

**Recht, den Datenschutzbeauftragten zu konsultieren** (Art. 38 DSGVO)
Betroffene Personen dürfen sich direkt an den Datenschutzbeauftragten des Verantwortlichen wenden und Fragen zu ihren personenbezogenen Daten stellen.

**Recht auf Beschwerde bei einer Aufsichtsbehörde** (Art. 77 DSGVO)
Ist die betroffene Person der Meinung, dass die Verarbeitung ihrer personenbezogenen Daten durch den Verantwortlichen oder einen Auftragsverarbeiter gegen ihre Rechte und Freiheiten verstößt, kann sie sich an die zuständige Aufsichtsbehörde wenden.

# Aufgaben des Staates

### Kontrolle

Die Datenschutz-Aufsichtsbehörden kontrollieren in Unternehmen und öffentlichen Stellen die Datenschutzorganisation, die Zulässigkeit der Verarbeitung und die Einhaltung der Rechte der betroffenen Personen. Zur Durchsetzung der DSGVO können sie Bußgelder verhängen, Auflagen erteilen und Datenverarbeitungen einschränken oder verbieten.

### Abstimmung auf europäischer Ebene

Die Datenschutz-Aufsichtsbehörden der jeweiligen EU-Mitgliedsstaaten sind im Europäischen Datenschutzausschuss vertreten. Dieser soll sicherstellen, dass die DSGVO in den EU-Mitgliedsstaaten einheitlich angewandt wird. Dazu soll der Ausschuss nach Maßgabe des Art. 70 DSGVO:

- zusätzlich zu den nationalen Datenschutzbehörden die ordnungsgemäße Anwendung der DSGVO überwachen und sicherstellen,
- die Europäische Kommission in Datenschutzfragen beraten,
- Leitlinien und Empfehlungen bereitstellen sowie
- den Austausch von Fachwissen und von Dokumentationen über Datenschutzvorschriften und -praxis mit Datenschutz-Aufsichtsbehörden in aller Welt fördern und abstimmen.

### Beratung

Die Datenschutz-Aufsichtsbehörden beraten Bürger, Unternehmen und öffentlichen Stellen, z. B. bei der Aufklärung zu datenschutzrechtlichen Pflichten oder auch bei der Klassifizierung von Datenverarbeitungsprozessen (Art. 57 Abs. 1 lit. d und k DSGVO).

# Sanktionen

### Konsequenzen für Unternehmen

Verstöße gegen die DSGVO sind bußgeldbewehrt und verpflichten den Verantwortlichen unter Umständen zu Schadenersatz. Außerdem besteht ein hohes Risiko von Reputationsschäden.

Art. 83 DSGVO erhöht den Bußgeldrahmen und führt konkrete Vorgaben für Abwägungskriterien bei der Verhängung von Bußgeldern ein. Bußgelder müssen unter anderem wirksam, verhältnismäßig und abschreckend sein. Im Einzelfall müssen die Aufsichtsbehörden bei der Entscheidung für oder gegen ein Bußgeld und über dessen Höhe bestimmte, in Art. 83 Abs. 2 DSGVO festgesetzte Kriterien berücksichtigen.

### Bußgelder

Bußgelder bis zu 20 Mio. Euro oder 4 % des Konzernumsatzes können verhängt werden bei:

- Verstoß gegen die Grundsätze der Verarbeitung und die Bedingungen für die Einwilligung (Art. 5, 6, 7 und 9),
- Verstoß gegen die Rechte der betroffenen Person (Art. 12 bis 22),
- Verstoß gegen die Übermittlung personenbezogener Daten an Empfänger in einem Drittland bzw. eine internationale Organisation (Art. 44 bis 49).

Bis zu 10 Mio. Euro oder 2 % des Konzernumsatzes können verhängt werden bei:

- Verstoß gegen die Pflichten des Verantwortlichen bzw. des Auftragsverarbeiters (Art. 8 Abs.1, Art. 25 bis 39, 42 und 43), z. B. Einwilligung von Kindern, Privacy by Design und Privacy by Default.

### Schadensersatz

Jede betroffene Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

**Bußgelder und Schadensersatz**

Die Höhe möglicher Bußgelder und Schadensersatzansprüche ist mit der DSGVO signifikant gestiegen. Auch damit unterstreicht der Gesetzgeber die hohe Bedeutung des Datenschutzes.

### Konsequenzen für Mitarbeiter

Auch Mitarbeitern droht neben arbeitsrechtlichen Konsequenzen von Abmahnung bis Kündigung unter Umständen eine Schadensersatzpflicht gegenüber dem Arbeitgeber, wenn er die Datenschutzpflichten nicht beachtet.

Vorsätzliche Handlungen durch rechtswidrige Datenverarbeitungen, die in Schädigungs- oder Bereicherungsabsicht oder gegen Entgelt begangen werden, sind Straftaten.

Sowohl betroffene Personen als auch das Unternehmen oder die Datenschutz-Aufsichtsbehörden können dies zur Anzeige bringen.

**Mitarbeiter in der Pflicht**

Mitarbeitern drohen

- arbeitsrechtliche Konsequenzen, aber auch
- Schadensersatzpflichten

bei Verstößen gegen die DSGVO.

Wenn Sie Zweifel haben, richtig zu handeln, hilft Ihnen Ihr Datenschutzbeauftragter weiter.

# Glossar

**Anonyme Daten/Anonymisierung**
Die Datenschutzgrundsätze gelten nicht für anonyme Informationen. Darunter sind

- Informationen zu verstehen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder
- personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Allerdings ist Vorsicht geboten, da sich eine Identifizierung (aufgrund der heutigen technischen Möglichkeiten) nur schwerlich ausschließen lässt. Anders ausgedrückt: Eine absolute Anonymität, wie sie implizit die DSGVO einfordert, ist kaum mehr möglich.

Übrigens: Während das alte BDSG den Begriff der Anonymisierung noch kannte, wird er im BDSG-neu nicht mehr definiert.

---

**Aufsichtsbehörde/Behörde**
Die Aufsichtsbehörden haben die Aufgabe, die Anwendung bzw. Umsetzung der DSGVO zu überwachen und auch durchzusetzen. Darüber hinaus haben sie die Öffentlichkeit für die Bestimmungen der DSGVO zu sensibilisieren und auch die Betroffenen unentgeltlich zu beraten. Datenschutz ist Landesaufgabe, zuständig sind die Landesdatenschutzbehörde.

---

**Auftragsverarbeiter/Auftragsverarbeitung**
Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet (DSGVO Art. 4).

Die Auftragsverarbeitung setzt zwingend einen Vertrag zur Auftragsverarbeitung voraus. Auch der Auftragnehmer ist haftbar. In dem Vertrag sollten unter anderem

- der Gegenstand, die Dauer sowie die Art und Weise der Verarbeitung,
- die Art der personenbezogenen Daten,
- die besonderen Aufgaben und Pflichten des Auftragsverarbeiters, insbesondere die Meldung von Datenpannen, aber auch die Unterstützung des Auftraggebers,
- die Durchführung einer Datenschutz-Folgenabschätzung sowie
- die Zusammenarbeit mit der Datenschutzaufsicht und ggf. dem Datenschutzbeauftragten definiert werden.

---

**Besonders sensible Daten/besondere Kategorien personenbezogener Daten**
Personenbezogene Daten, die ihrem Wesen nach besonders sensibel sind, verdienen einen besonderen Schutz. Die Verarbeitung personenbezogener Daten, aus denen

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit

hervorgehen, sowie die Verarbeitung von

- genetischen oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder
- der sexuellen Orientierung einer natürlichen Person

ist laut Art. 9 DSGVO grundsätzlich untersagt.
Es gibt Ausnahmen. Sie bedürfen jedoch einer gezielten gesetzlichen Rechtfertigungsnorm.

---

**Betroffener/betroffene Person**
Der Betroffene ist derjenige, dessen personenbezogene Daten verarbeitet werden. Synonyme zu „Betroffener" bzw. „betroffene Person" sind die natürliche Person oder auch das Datensubjekt.

---

**Bundesdatenschutzgesetz**
Das neue Bundesdatenschutzgesetz (BDSG-neu) umfasst

- allgemeine Regeln zur Verarbeitung personenbezogener Daten auf Basis der DSGVO,
- ergänzende Regelungen zur DSGVO,
- Regeln zur Umsetzung der EU-Datenschutzrichtlinie für Polizei und Justiz sowie

- Spezialregelungen für Behörden des Bundesministeriums der Verteidigung.

---

**Dateisystem**

Die DSGVO (Art. 4) definiert ein Dateisystem als eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist. Dabei ist es egal, ob die Sammlung

- zentral oder dezentral,
- nach funktionalen Gesichtspunkten geordnet oder
- nach geografischen Gesichtspunkten geordnet

geführt wird.

---

**Datenminimierung (Verarbeitungsgrundsatz)**

Der Grundsatz der Datenminimierung besagt, dass personenbezogene Daten sparsam erhoben werden müssen. Die Erhebung muss dem jeweiligen Zweck „angemessen" und auf das „notwendige Maß" beschränkt sein (DSGVO Art. 5 Abs. lit. c).

---

**Datenschutzbeauftragter**

Zu den Aufgaben des Datenschutzbeauftragten gehört, datenschutzrelevante Risiken im Blick zu haben, die Geschäftsführung (bzw. den Verantwortlichen im Sinne der DSGVO) zu beraten, die Umsetzung der gesetzlichen Vorgaben zu beachten, mit Behörden zusammenzuarbeiten und vor allem Ansprechpartner für das verantwortliche Unternehmen und dessen Mitarbeitern im Datenschutz zu sein.

---

**Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen / Privacy by Design, Data Protection by Default**

Für den Schutz personenbezogener Daten sind rechtzeitig geeignete technische und organisatorische Maßnahmen (sogenannte TOM) vorzunehmen.

Der Grundsatz „Datenschutz durch Technikgestaltung" (Privacy oder auch Data Protection by Design) besagt, dass die Datenschutzanforderungen bereits bei der Anwendungsentwicklung mitzubedenken sind.

„Datenschutzfreundliche Voreinstellungen" (Privacy oder auch Data Protection by Default) meint die technische Sicherstellung der zweckgebundenen Verarbeitung personenbezogener Daten. Das bezieht sich auf die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Ein Zertifizierungsverfahren (gem. Art. 42 DSGVO) kann als Nachweis herangezogen werden.

---

**Datenschutz-Grundverordnung/DSGVO**

Die EU-Datenschutz-Grundverordnung (DSGVO) regelt auf europäischer Ebene den Datenschutz. Auf nationaler Ebene muss bzw. darf der Gesetzgeber ergänzende und detailliertere Vorschriften erlassen („Öffnungsklauseln", deshalb auch Grund-Verordnung).

Die DSGVO regelt die Verarbeitung personenbezogener Daten. Der Begriff „Verarbeitung" meint unter anderem

- das Abfragen, den Abgleich, die Ablage, das Auslesen, die Archivierung, die Bereitstellung, die Bildschirmdarstellung, die Einschränkung, die Erfassung, die Erhebung, die Erweiterung, die Katalogisierung, die Lagerung, die Löschung, das Ordnen, die Organisation, die Speicherung, die Strukturierung, die Systematisierung, die Übermittlung, die Veränderung, die Verbreitung, die Verknüpfung, die Vernichtung, den Versand von Daten.

Dabei ist es egal, ob

- die Verarbeitung mit oder ohne Hilfe automatisierter Verfahrenen stattfindet und ob
- die Verarbeitung online oder offline erfolgt.

Datenbanken, elektronische Dokumente, papierhafte Akten und Karteikarten fallen ebenso unter die DSGVO wie Audiodateien oder Telefon- und Videoaufzeichnungen.

Die Verarbeitung personenbezogener Daten ist dabei so lange verboten, bis sie – ausdrücklich oder durch Erlaubnistatbestand – erlaubt wurde. Die Einwilligung zur Verarbeitung personenbezogener Daten muss freiwillig geschehen und kann schriftlich, elektronisch oder mündlich erteilt werden. In jedem Fall muss aufgrund der Nachweispflicht des Verantwortlichen die Einwilligung dokumentiert werden.

**Dokumentation**
Die DSGVO spricht nicht von einer Dokumentationspflicht, sondern von einer Nachweispflicht. Das heißt, die ordnungsgemäße Datenverarbeitung personenbezogener Daten ist nachzuweisen. Dabei ist auch die Dokumentation, beispielsweise in einem Verzeichnis der Verarbeitungstätigkeiten, wichtig.

---

**Geltungsbereich der EU-DSGVO**
Von der DSGVO sind praktisch alle Unternehmen betroffen, die innerhalb der EU personenbezogene Daten von Kunden oder anderen Personen in ihrem Umfeld erheben, verarbeiten oder nutzen. Auch Unternehmen, die ihren Hauptsitz außerhalb der EU haben, innerhalb der Gemeinschaft aber Waren oder Dienstleistungen vertreiben, unterliegen den Regelungen der DSGVO.
Beispiele:
- Selbständige
- Vereine
- Produktions-, Handels- und Dienstleistungsunternehmen
- Anbieter sozialer Netzwerke (Twitter, Facebook, Instagram etc.)
- Rechenzentren
- Auskunfteien
- Markt- und Meinungsforscher
- Adresshändler und -verlage
- wissenschaftliche Forschungseinrichtungen
- Medien
- Bundesbehörden
- Kommunalverwaltung

---

**Haftung/Recht auf Schadensersatz**
„Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde." (Art. 82 DSGVO)

**Identifiziert/Identifizierbar**
Die Eigenschaften „identifiziert" und „identifizierbar" beziehen sich auf die zu schützende Person bzw. den Betroffenen. Sobald der Betroffene – direkt oder indirekt – identifiziert werden kann, fällt die Datenverarbeitung unter die Bestimmungen der DSGVO. Dabei ist unerheblich, ob die Daten auf die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität der natürlichen Person verweisen.

---

**Integrität und Vertraulichkeit (Verarbeitungsgrundsatz)**
Der Grundsatz der Integrität und Vertraulichkeit besagt, dass die Verarbeitung eine angemessene Sicherheit der personenbezogenen Daten gewährleisten muss (DSGVO Art. 5 Abs. 1 lit. f).

---

**Interessenabwägung**
Der Erwägungsgrund 47 besagt, dass der Verantwortliche, beispielsweise Ihr Unternehmen, Daten dann verarbeiten darf, wenn
- er ein „berechtigtes Interesse" begründen kann und
- die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Darüber hinaus ist darauf zu achten, ob für den Betroffenen die Datenverarbeitung zu erwarten, das heißt absehbar ist.

---

**Marketingaktionen**
Die Durchführung von Direktmarketing oder auch Online-Marketing wird im Erwägungsgrund 47 als berechtigtes Interesse betrachtet. Dafür hat aber der Betroffene ein bedingungsloses Widerspruchsrecht (siehe auch Interessenabwägung).

**Personenbezogene Daten**
Personenbezogene Daten sind nach Art. 4 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
Zu den geschützten Informationen gehören z. B. Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Bankverbindungen.

Als „identifizierbar" wird eine natürliche Person angesehen, die – direkt oder indirekt – identifiziert werden kann, beispielsweise mittels Zuordnung zu

- einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder einer Online-Kennung oder auch zu
- besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Abgrenzung: Juristische Personen wie auch die Daten Verstorbener sind nicht durch die DSGVO geschützt. Auch anonymisierte Daten fallen nicht unter die DSGVO.

---

**Profiling**
Profiling im Sinne der DSGVO meint die automatisierte Datenverarbeitung, um bestimmte Aspekte einer Person zu bewerten. Die DSGVO nennt dabei unter anderem die Analyse und Vorhersage von Arbeitsleistungen, der wirtschaftlichen Lage, der Gesundheit, von Interessen oder auch des Aufenthaltsortes.

---

**Pseudonymisierung**
Die Pseudonymisierung meint die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Diese zusätzlichen Informationen sollten gesondert aufbewahrt werden. Darüber hinaus sollen sie technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können (DSGVO Art. 4).

**Rechenschaftspflicht, Nachweispflicht (Verarbeitungsgrundsatz)**
Der Grundsatz der Rechenschaftspflicht besagt, dass der Verantwortliche für die ordnungsgemäße Verarbeitung der Daten rechenschafts- und nachweispflichtig ist. Letztlich impliziert dieser Grundsatz eine umfassende Dokumentation aller datenverarbeitenden Tätigkeiten (DSGVO Art. 5 Abs. 2).

---

**Richtigkeit (Verarbeitungsgrundsatz)**
Der Grundsatz der Richtigkeit besagt, dass die Daten sachlich richtig (entsprechend dem Zweck) sein müssen und erforderlichenfalls auf den neuesten Stand zu bringen sind. Unrichtige Daten sind unverzüglich zu löschen oder zu berichtigen (DSGVO Art. 5 Abs. 1 lit. d).

---

**Speicherbegrenzung (Verarbeitungsgrundsatz)**
Der Grundsatz der Speicherbegrenzung besagt, dass personenbezogene Daten nur so lange gespeichert werden dürfen, wie es für den jeweiligen Zweck erforderlich ist (DSGVO Art. 5 Abs. 1 lit. e).

---

**Treu und Glauben, Transparenz (Verarbeitungsgrundsatz)**
Der Grundsatz „nach Treu und Glauben" besagt, dass personenbezogene Daten ausschließlich so verarbeitet werden dürfen, wie es bei der Erhebung angegeben wurde. Die Verarbeitung darf darüber hinaus nur in dem Umfang erfolgen, auf den der Betroffene „vertrauen" darf und soweit sie für ihn nachvollziehbar ist (DSGVO Art. 5 Abs. 1 lit. a).

---

**Verantwortlicher**
Ein Verantwortlicher im Sinne der DSGVO (Art. 4) ist eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle", die über eine Verarbeitung personenbezogener Daten entscheidet. Dabei ist es egal, ob er alleine oder gemeinsam mit anderen die Entscheidung trifft.

**Verarbeitungsgrundsätze**

- Treu und Glauben, Transparenz (DSGVO Art. 5 Abs. 1 lit. a)
- Zweckbindung (DSGVO Art. 5 Abs. lit. b)
- Datenminimierung (DSGVO Art. 5 Abs. 1 lit. c)
- Richtigkeit (DSGVO Art. 5 Abs. 1 lit. d)
- Speicherbegrenzung (DSGVO Art. 5 Abs. 1 lit. e)
- Integrität und Vertraulichkeit (DSGVO Art. 5 Abs. 1 lit. f)
- Rechenschaftspflicht (DSGVO Art. 5 Abs. 2)

---

**Verbotsprinzip**

Die Verarbeitung personenbezogener Daten ist dabei so lange verboten, bis sie – ausdrücklich oder durch Erlaubnistatbestand – erlaubt wurde.

---

**Zertifizierung**

Die DSGVO sieht ein Zertifizierungsverfahren sowie Datenschutzprüfzeichen vor, die dazu dienen, nachzuweisen, dass die Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird (DSGVO Art. 42).

---

**Zweckbindung (Verarbeitungsgrundsatz)**

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen (DSGVO Art. 5 Abs. 1 lit. b).

## IMPRESSUM

**Beileger der Point of Compliance 2/2018** · **Herausgeber:** GenoTec GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.geno-tec.de Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917, Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter · **Verantwortlich i. S. d. P. :** Jens Saenger · **Redaktion:** Gabriele Seifert, Leitung (red.) · **Redaktionsanschrift:** GenoTec GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@geno-tec.de · **Bildnachweise:** © iStockphoto, Rawpixel · **Gestaltung:** EGENOLF DESIGN, Wiesbaden, studio@egenolf-design.de **Druck:** odd GmbH & Co. KG · Print und Medien www.odd.de · **Redaktioneller Hinweis:** Nachdruck, auch auszugsweise, nur mit ausdrücklicher Genehmigung der Redaktion sowie mit Quellenangabe und gegen Belegexemplar. Die Beiträge sind urheberrechtlich geschützt. Zitate sind mit Quellenangabe zu versehen. Jede darüber hinausgehende Nutzung, wie die Vervielfältigung, Verbreitung, Veröffentlichung und Onlinezugänglichmachung des Magazins oder einzelner Beiträge aus dem Magazin, stellt eine zustimmungsbedürftige Nutzungshandlung dar. Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung des Herausgebers wieder. Die GenoTec GmbH übernimmt keinerlei Haftung für die Richtigkeit des Inhalts. · **Redaktionsschluss:** 17. September 2018 · **Auflage:** 3.000 Exemplare. Die aktuellen Mediadaten finden Sie im Internet unter www.geno-tec.de/poc.

# Kontakt

**Datenschutzbeauftragter**
Die Kontaktdaten der Datenschutzbeauftragten in den Bundesländern finden Sie unter anderem auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter:
www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

---

**GenoTec GmbH**
Tel. 069 6978-3324
E-Mail datenschutz@geno-tec.de
www.geno-tec.de